CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2026/41

I – Objeto

1. A Presidente da Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias da Assembleia da República solicitou à Comissão Nacional de Proteção de Dados (CNPD) que se pronunciasse sobre a Proposta de Lei n.º 83/XXV/2026, que transpõe para a ordem jurídica interna a Diretiva (UE) 2023/1544, relativa à designação de estabelecimentos designados e de representantes legais de prestadores de serviços para efeitos de obtenção de prova eletrónica, e estabelece o regime sancionatório aplicável ao incumprimento das obrigações decorrentes da referida Diretiva e do Regulamento (UE) 2023/1543.
2. A presente pronúncia é emitida ao abrigo do disposto no artigo 43.º, n.º 1, e no artigo 44.º, n.º 1, alíneas a) e c), da Lei n.º 59/2019, de 8 de agosto, enquanto autoridade nacional de controlo competente no domínio da proteção de dados pessoais tratados para fins de prevenção, investigação, deteção e repressão de infrações penais.

II – Enquadramento geral

3. Na era digital, estima-se que, na União Europeia, 85% das investigações criminais recorram a dados que se encontram em ambiente digital, como se diz no Preâmbulo da Proposta de Lei.
4. O regime europeu em análise (cf. Regulamento (UE) 2023/1543 e Diretiva (UE) 2023/1544) institui um modelo inovador de obtenção de prova eletrónica, permitindo que autoridades judiciais de um Estado-membro dirijam ordens diretamente a prestadores de serviços, independentemente da localização dos dados.
5. Este modelo distingue-se claramente do regime anteriormente vigente, nomeadamente da Diretiva 2006/24/CE (Lei n.º 32/2008), baseada na conservação preventiva e generalizada de dados, passando para um sistema de obtenção e conservação dirigida de dados já existentes, no âmbito de processos penais concretos (cf. o novo regime europeu nasce precisamente porque o modelo da retenção massiva foi sucessivamente censurado pelo TJUE no Acórdão do Tribunal de Justiça (Grande Secção) de 8 de abril de 2014, EU:C:2014:238, Processos apensos C-293/12 e C-594/12 [Digital Rights Ireland], no Acórdão do Tribunal de Justiça (Grande Secção) de 21 de dezembro de 2016, EU:C:2016:970, Processos apensos C-203/15 e C-698/15 [Tele2 Sverige] e Acórdão do Tribunal de Justiça (Grande Secção) de 6 de outubro de 2020, EU:C:2020:79, Processos apensos C-511/18, C-512/18 e C-520/18 [La Quadrature du Net]).

6. Importa sublinhar que o Regulamento (UE) 2023/1543 é diretamente aplicável e que a Diretiva impõe um resultado obrigatório, sendo, por isso, o espaço de intervenção do legislador nacional de natureza essencialmente organizatória e sancionatória, não estrutural.

III – Apreciação

1. Da ausência de avaliação de impacto sobre a proteção de dados

7. O pedido não vem acompanhado por uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), não cumprindo o disposto no n.º 4 do artigo 18.º da Lei n.º 43/2004, de 18 de agosto, na redação introduzida pela Lei n.º 58/2019, de 8 de agosto, segundo o qual os pedidos de parecer relativos a disposições legais e regulamentares em preparação devem ser remetidos à Comissão Nacional de Proteção de Dados instruídos com o respetivo estudo de impacto sobre a proteção de dados.
8. Nos termos do artigo 35.º do RGPD, deve ser realizada uma avaliação de impacto sobre a proteção de dados sempre que um tipo de tratamento, em especial recorrendo a novas tecnologias, seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares.
9. Invoca-se aqui o artigo 35.º do RGPD como parâmetro substantivo e não como base direta de obrigatoriedade procedimental.

2. Natureza das ordens europeias e princípio da minimização

10. O Regulamento não consagra a existência de obrigação de conservação generalizada e consagra a distinção entre ordens de produção (dados existentes) e ordens de conservação (preservação temporária).
11. Este modelo é, em si, coerente com o princípio da minimização dos dados (artigo 5.º, n.º 1, alínea c), do RGPD), na medida em que limita o acesso a dados estritamente necessários, afasta a criação de reservas massivas de informação e impõe uma lógica de intervenção casuística e proporcional.
12. Todavia, a efetividade desse princípio depende da sua concretização na emissão das ordens, na execução pelos prestadores e no tratamento subsequente pelas autoridades.

3. Enquadramento na Lei n.º 59/2019, de 8 de agosto (Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações

penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016)

13. O tratamento de dados pessoais efetuado no âmbito desta Proposta de regime legal insere-se no domínio da investigação criminal, sendo aplicável a Lei n.º 59/2019.
14. Devem, por isso, ser respeitados os princípios gerais da proteção de dados do artigo 4.º da referida Lei n.º 59/2019.
15. A Proposta de Lei deve ser lida em articulação sistemática com este regime, sob pena de lacunas na proteção efetiva dos dados.

4. Acessos seguros e integridade dos dados

16. O artigo 10.º, n.º 2, da Proposta de Lei, ao tipificar como contraordenação a não adoção das medidas técnicas e operacionais previstas no artigo 13.º, n.º 4, do Regulamento (UE) 2023/1543 (segundo o qual os destinatários devem adotar as medidas mais avançadas necessárias para garantir a confidencialidade, o sigilo e a integridade das ordens e dos dados), evidencia a importância da salvaguarda da segurança da informação no âmbito do presente regime.
17. Todavia, a consagração de um ilícito contraordenacional, em sede de imputação objetiva, com base numa remissão para um conceito aberto e evolutivo suscita reservas à luz do princípio da tipicidade, na vertente da determinabilidade das infrações, na medida em que pode comprometer a previsibilidade das condutas exigidas aos destinatários.
18. O problema não é a obrigação europeia (que é inevitavelmente aberta), mas antes a sua transposição sancionatória sem densificação suficiente.
19. Adicionalmente, e sem prejuízo da necessidade de manter a flexibilidade inerente à evolução tecnológica, a CNPD considera desejável uma maior densificação normativa ao nível interno, designadamente através da explicitação de critérios ou parâmetros orientadores quanto às medidas a adotar.
20. Nesse contexto, sugere-se prever a necessidade de adoção de soluções técnicas adequadas ao estado da técnica, incluindo, nomeadamente mecanismos de autenticação robusta, encriptação das comunicações e registo e auditoria de acessos.
21. Tal densificação reforçará a segurança jurídica dos destinatários e assegurará uma aplicação mais previsível e proporcional do regime sancionatório.

5. Conservação de dados e enquadramento do ciclo de vida dos dados

22. A Proposta de Lei designa a Autoridade Nacional de Comunicações (ANACOM) como autoridade central responsável pela recolha, organização e tratamento da informação relativa aos estabelecimentos designados e aos representantes legais dos prestadores de serviços.
23. Neste contexto, importa sublinhar que tais atividades configuram operações de tratamento de dados pessoais para efeitos de prevenção, investigação, deteção e repressão de infrações penais, sendo, nessa medida, aplicável o regime da Lei n.º 59/2019, de 8 de agosto.
24. Ora, nos termos deste regime, o tratamento de dados pessoais por autoridades públicas deve assentar em base jurídica clara, precisa e suficientemente densificada, designadamente no que respeita a: *(i)* finalidades do tratamento; *(ii)* categorias de dados tratados; *(iii)* prazos de conservação; e *(iv)* condições de acesso, controlo e segurança.
25. Não obstante a definição funcional da ANACOM como autoridade central, a Proposta de Lei não explicita, com o nível de detalhe exigido, os parâmetros relativos ao ciclo de vida dos dados pessoais objeto de tratamento, em particular quanto à sua conservação, atualização e eliminação.
26. Acresce que, no ordenamento jurídico nacional, o regime de conservação de dados judiciais em formato eletrónico apresenta um nível de densificação limitado. Com efeito, a Lei n.º 34/2009, de 14 de julho (alterada pela Lei n.º 30/2017, de 30 de maio), estabelece no seu artigo 40.º, n.º 4, que a eliminação dos dados arquivados eletronicamente se rege pelos diplomas que regulam o arquivamento e a destruição de processos e documentos judiciais, com as necessárias adaptações.
27. Todavia, o Regulamento de Conservação Arquivística dos Tribunais Judiciais e dos Tribunais Administrativos e Fiscais, aprovado pela Portaria n.º 368/2013, de 24 de dezembro, foi concebido num contexto essencialmente analógico, sendo apenas adaptados à realidade digital, não definindo, de forma específica e sistemática, critérios próprios para a conservação e eliminação de dados eletrónicos.
28. Além do mais, verifica-se, na prática, que apesar da eliminação de dados em processos em papel, os mesmos continuam disponíveis na plataforma Citius, ainda que com limitações de acesso, o que levanta problemas, por exemplo, à luz do princípio da limitação da conservação (artigo 5.º, n.º 1, alínea e), do RGPD)[1].

[1] No Acórdão do TEDH de 04/12/2008 (Requerimentos (Applications) n.ºs 30562/04 e 30566/04; Marper) o Tribunal considerou que a retenção indefinida das impressões digitais, amostras de células e perfis de ADN era desproporcionada e desnecessária numa sociedade democrática, considerando que o processo penal tinha terminado com uma absolvição:

> *«125. O Tribunal considera que a natureza geral e indiferenciada do poder de retenção de impressões digitais, amostras biológicas e perfis de DNA de pessoas suspeitas de terem cometido crimes, mas não condenadas, conforme aplicado aos requerentes no presente caso, não reflete um equilíbrio justo entre os interesses públicos e privados concorrentes em jogo, e que o Estado demandado excedeu qualquer margem*

29. Por seu turno, o regime da tramitação eletrónica dos processos judiciais, aprovado pela Portaria n.º 280/2013, de 26 de agosto, não estabelece prazos autónomos de conservação ou eliminação aplicáveis aos processos em formato digital.
30. Neste contexto, a ausência de um regime densificado e especificamente adaptado à realidade digital pode gerar incerteza quanto à duração da conservação dos dados obtidos ao abrigo do sistema *e-evidence*, bem como quanto às condições da sua eliminação.
31. A CNPD considera, por isso, que a definição de regras claras quanto ao ciclo de vida dos dados — designadamente no que respeita à sua conservação, atualização e eliminação — constitui elemento essencial para assegurar a conformidade do regime com o quadro jurídico nacional e europeu de proteção de dados, em particular com os princípios da limitação das finalidades, da minimização dos dados, da limitação da conservação, e da integridade e confidencialidade (artigo 5.°, alíneas b), c), e) e f) do RGPD).
32. Em especial, revela-se desejável que o legislador densifique, direta ou indiretamente, os critérios aplicáveis à conservação dos dados obtidos no âmbito das ordens europeias, assegurando a sua adequada articulação com o direito processual penal e com o regime arquivístico vigente, que deve ser atualizado para a realidade digital.
33. A CNPD sublinha que este problema não se esgota no âmbito da presente Proposta de Lei, antes refletindo uma insuficiente adaptação do regime jurídico nacional de conservação e eliminação de dados à realidade digital.
34. Neste sentido, a definição de critérios claros aplicáveis aos dados obtidos através de ordens europeias revela-se não apenas necessária para a execução da presente Proposta de Lei, mas também para assegurar uma coerência sistemática em sede de tratamento de dados pessoais no âmbito dos processos judiciais em ambiente digital.
35. Convém recordar que as COEP e COEC vão fazer entrar nos processos judiciais e do Ministério Público volumes significativos de prova eletrónica.

---

de apreciação permitida nesta área. Portanto, a retenção impugnada constitui uma interferência desproporcional no direito dos requerentes ao respeito pela sua vida privada e não pode ser considerada necessária numa sociedade democrática…[…].

126. Consequentemente, houve uma violação do artigo 8.º da Convenção no presente caso.»

No Acórdão do TEDH de 06/06/2006 (SEGERSTEDT-WIBERG ET AUTRES c. SUÈDE; - Requerimento (Application) n.º 62332/00), o Tribunal constatou uma violação do art.º 8.º da CEDH uma vez que o armazenamento contínuo de dados não era pertinente, devido ao longo período decorrido (cf. ingerência desproporcionada no exercício do direito ao respeito pela vida privada).

36. Estamos perante uma Proposta de Lei cuja finalidade última é a obtenção, conservação e utilização de prova eletrónica em processos penais e de execução de penas. A própria Proposta de Lei remete expressamente para o Regulamento e-Evidence e altera a Lei da Cooperação Judiciária Internacional e a Lei do Cibercrime.

6. Conservação de dados pelos prestadores

37. O regime sanciona a não conservação de dados no âmbito de certificado de ordem europeia de produção (COEP) ou no âmbito do certificado de ordem europeia de conservação (COEC).
38. Importa, no entanto, clarificar que a conservação de dados apenas pode ocorrer nos estritos termos da ordem de conservação, sendo limitada no tempo e finalidade.
39. Recomenda-se evitar interpretações que reintroduzam, ainda que indiretamente, obrigações generalizadas de retenção.

7. Comunicações e formas de transmissão (artigo 6.º)

40. A Proposta de Lei prevê comunicações diretas entre autoridades judiciárias e prestadores de serviços ou respetivos representantes legais, em conformidade com o modelo instituído pelo Regulamento (UE) 2023/1543.
41. Tal solução, embora funcionalmente adequada à celeridade exigida na obtenção de prova eletrónica, implica riscos relevantes, designadamente quanto à segurança das transmissões, identificação inequívoca do destinatário e prevenção de acessos indevidos.
42. A CNPD entende que a Proposta de Lei não densifica suficientemente os requisitos técnicos associados a estas comunicações, não obstante a sensibilidade dos dados em causa e o caráter transfronteiriço das operações.
43. Neste contexto, importa notar que, a nível da União Europeia, têm sido desenvolvidas iniciativas destinadas a apoiar as autoridades na gestão segura e eficaz do acesso a prova eletrónica, como o projeto SIRIUS, implementado pela Europol e pela Eurojust, que funciona como ponto de referência para a partilha de boas práticas e conhecimento especializado neste domínio.
44. Sem prejuízo de tais instrumentos operacionais, a CNPD considera que o quadro normativo nacional deve assegurar, de forma autónoma, a definição de garantias mínimas quanto à segurança das comunicações, designadamente através da previsão de: *(i)* mecanismos de autenticação forte das entidades intervenientes; *(ii)* utilização de canais de transmissão seguros e, sempre que adequado, encriptados; e *(iii)* sistemas de registo e rastreabilidade das comunicações efetuadas,

tendo em vista assegurar a adequada proteção de dados pessoais, aumentar a confiança no sistema e reduzir o risco de incumprimento decorrente de falhas técnicas ou operacionais.

45. Em particular, importa garantir que os mecanismos de comunicação adotados asseguram um nível de segurança adequado ao risco, tendo em conta a natureza dos dados tratados e o contexto transfronteiriço das operações.

8. Publicação de informação (artigo 9.º, n.º 5)

46. Prevê-se a comunicação e publicação de informações sobre estabelecimentos designados e representantes legais.
47. Esta divulgação deve respeitar os princípios da limitação das finalidades e da minimização dos dados (artigo 5.°, alíneas b) e c) do RGPD).
48. Deve evitar-se a exposição excessiva de dados identificativos e/ou a reutilização indevida da informação publicada.

9. Celeridade e controlo

49. O regime instituído pelo Regulamento (UE) 2023/1543 assenta na definição de prazos particularmente curtos para a execução das ordens europeias de produção e de conservação, designadamente no que respeita à resposta dos destinatários e à eventual intervenção do Estado de execução (cf. artigo 12.º do Regulamento).
50. Tal solução visa assegurar a eficácia da investigação penal, tendo em conta a natureza volátil da prova eletrónica e o risco de perda irreversível de dados.
51. Todavia, a compressão dos prazos de resposta e de reação pode ter como efeito uma redução da densidade do controlo em fase inicial, nomeadamente no que respeita à apreciação da necessidade, proporcionalidade e conformidade da medida com os direitos fundamentais.
52. Neste contexto, o equilíbrio entre celeridade e garantias desloca-se, em parte, para momentos posteriores à execução da ordem, assumindo particular relevância *(i)* os mecanismos de oposição previstos no artigo 12.º do Regulamento, que permitem ao Estado de execução invocar fundamentos materiais de recusa, designadamente com base na proteção de direitos fundamentais; *(ii)* os mecanismos de tutela jurisdicional efetiva, nos termos do artigo 18.º do Regulamento, assegurando a possibilidade de controlo judicial subsequente; e *(iii)* o regime de tratamento de dados pessoais previsto na Lei n.º 59/2019, designadamente no que respeita aos princípios da limitação das finalidades, minimização, conservação e controlo de acesso.

53. Neste quadro, a CNPD considera que a Proposta de Lei deve ser interpretada e, na medida do possível, densificada no sentido de reforçar os mecanismos de controlo subsequente, designadamente através de:
    a) Definição clara de regras quanto ao registo e rastreabilidade das operações de acesso, transmissão e tratamento de dados;
    b) Previsão de mecanismos de auditoria interna e, quando aplicável, externa das entidades envolvidas;
    c) Aplicação rigorosa de critérios de conservação e eliminação dos dados obtidos, nos termos da Lei n.º 59/2019; e
    d) Reforço da documentação e fundamentação das decisões de tratamento de dados, em linha com o princípio da responsabilidade (accountability).
54. Tais mecanismos revelam-se particularmente relevantes no domínio regulado pela Lei n.º 59/2019, atendendo ao disposto nos artigos 27.º e 31.º da mesma Lei, relativos ao registo cronológico das operações de tratamento e à segurança do tratamento.
55. Adicionalmente, entende-se que a articulação entre o regime europeu e o direito processual penal interno — designadamente no que respeita à intervenção do juiz de instrução nos casos exigidos e à fiscalização jurisdicional subsequente — constitui elemento essencial para compensar a menor densidade do controlo em fase inicial.
56. Tal articulação permite assegurar que a menor densidade do controlo em fase inicial é compensada por mecanismos de controlo jurisdicional e de garantia subsequente, mantendo-se o equilíbrio entre a exigência de eficácia e a proteção dos direitos fundamentais.
57. Em particular, importa assegurar que a celeridade na obtenção dos dados não se traduza numa extensão indevida da sua conservação ou reutilização para finalidades diversas, devendo ser rigorosamente observados os princípios da limitação da finalidade e da minimização.

IV — Conclusão

58. A CNPD recomenda:
    a) A definição de requisitos técnicos de segurança, incluindo no acesso, transmissão e tratamento de dados;
    b) A delimitação dos prazos e critérios de conservação dos dados, designadamente no ciclo de vida subsequente à sua obtenção;
    c) A definição clara do regime de tratamento de dados pela autoridade central (ANACOM);

d) O reforço dos mecanismos de controlo subsequente, nomeadamente através de auditoria, rastreabilidade e documentação das operações de tratamento.

59. A CNPD sublinha, em particular, que as lacunas identificadas no que respeita à conservação e eliminação de dados eletrónicos não se limitam ao âmbito da presente Proposta de Lei, refletindo antes uma insuficiente adaptação do regime jurídico nacional à realidade digital, designadamente no domínio do tratamento de dados pessoais em sede judicial.
60. A CNPD recomenda assim que, em sede de aprovação final do diploma, sejam introduzidas ou densificadas as seguintes soluções:

a) Quanto à segurança e transmissão de dados: explicitação de requisitos técnicos mínimos de segurança, designadamente: *(i)* autenticação forte das entidades intervenientes; *(ii)* utilização de canais de comunicação seguros e, quando adequado, encriptados; *(iii)* mecanismos de registo e auditoria das operações (rastreabilidade);

b) Relativamente à conservação e ciclo de vida dos dados: importa assegurar a definição de critérios claros quanto *(i)* aos prazos de conservação e *(ii)* às condições de acesso, atualização e eliminação dos dados, assegurando a articulação com a a Lei n.º 59/2019, de 8 de agosto e o regime arquivístico nacional, cuja adaptação à realidade digital se revela necessária; é relevante ainda nesta sede a introdução de mecanismos de obtenção transfronteiriça de prova eletrónica torna particularmente relevante a existência de regras claras quanto à conservação, atualização, acesso e eliminação dos dados obtidos, matéria que não se encontra plenamente densificada no ordenamento jurídico nacional, sobretudo em ambiente digital;

c) No regime sancionatório: importa clarificar os critérios de imputação da responsabilidade às pessoas singulares, assegurando *(i)* a verificação de culpa; *(ii)* a distinção entre funções de decisão e funções meramente executivas; *(iii)* a exclusão de imputações automáticas; e ao tipificar como contraordenação a não adoção das medidas técnicas e operacionais previstas no artigo 13.º, n.º 4, do Regulamento (UE) 2023/1543 (segundo o qual os destinatários devem adotar as medidas mais avançadas necessárias para garantir a confidencialidade, o sigilo e a integridade das ordens e dos dados), consagra-se um ilícito contraordenacional com base numa remissão para um conceito aberto e evolutivo, o que suscita reservas à luz do princípio da tipicidade, na vertente da determinabilidade das infrações, na medida em que pode comprometer a previsibilidade das condutas exigidas aos destinatários.

d) E quanto ao controlo e garantias subsequentes: recomenda-se o reforço dos mecanismos de controlo subsequente, designadamente através de auditorias internas e externas, documentação das decisões de tratamento e aplicação rigorosa dos princípios da limitação da finalidade e da minimização; e sempre tendo em conta que a celeridade do sistema não se pode traduzir em conservação excessiva de dados, ou reutilização para finalidades incompatíveis.

Lisboa, 8 de junho de 2026

José Mário Nogueira da Costa (Vogal)

Assinado por: **JOSÉ MÁRIO NOGUEIRA DA COSTA**
Num. de Identificação: 08325550
Data: 2026.06.08 18:16:35+01'00'

CARTÃO DE CIDADÃO